JC09 Rec'd PCT/PTO 14 JUN 2001

Form P10-1390
(rev 11-2000)

Express Mail No. EL280660416US

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER	U.S. APPLICATION NO. (if known, see 37 CFR 1.5)
NCX-002 (6909/3)	09/868151

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR99/03097	December 10, 1999	December 14, 1998

TITLE OF INVENTION
Method of Transporting Packets Between an Access Interface of a Subscriber Installation and a Shared Network, and Access Interface Implementing Such Method

APPLICANT FOR DO/EO/US
Hersent, Olivier

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9), and (21) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☒ is attached hereto.(along with a statement/declaration verifying the accuracy of the translation)
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(C)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(C)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98. (including 1 PTO 1449 form and Refs. A1, B1-B2, C1-C5).
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821-1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information: Inventor Data Sheet; copy of International preliminary Examination Report under PCT Article 36; copy of International Search Report; copy of Request; Formal Drawings (3 sheets) and return receipt postcard.

JC03 Rec'd PCT/PTO 14 JUN 2001

U.S. APPLICATION NO. (if known, see 37 CFR 1.5) 09/868151	INTERNATIONAL APPLICATION NO. PCT/FR99/03097	ATTORNEY'S DOCKET NUMBER NCX-002

21. ☒ The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a)(1) – (5)):

	CALCULATIONS PTO USE ONLY
Neither international preliminary examination fee (37 CFR 1,482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$860.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**	
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**	
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**	

ENTER APPROPRIATE BASIC FEE AMOUNT =				**$860.00**	
Surcharge of **$130.00** for furnishing the oath or declaration of later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				$	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	10 - 20 =	0	X **$18.00**	**0.00**	
Independent claims	2 - 3 =	0	X **$80.00**	**0.00**	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$270.00**	**$**	
TOTAL OF ABOVE CALCULATIONS =				**$860.00**	
☐ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.				**$0.00**	
SUBTOTAL =				**$0.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				**$**	
TOTAL NATIONAL FEE =				**$0.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				**$**	
TOTAL FEES ENCLOSED =				**$860.00**	
				Amount to be: refunded	$
				charged:	$

a. ☒ A check in the amount of $860.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 20-0531. A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Direct all correspondence to:

Patent Administrator
Testa, Hurwitz & Thibeault, LLP
High Street Tower
125 High Street
Boston, MA 02110
Tel. No.: (617) 248-7000
Fax No.: (617) 248-7100

Pat RH Wall 6/14/01

SIGNATURE

Patrick R.H. Waller

NAME

41,418

REGISTRATION NUMBER

09/868151
Express Mail Label No. EL280660416US
JC03 Rec'd PCT/PTO 14 JUN 2001

PATENT
Attorney Docket No. NCX-002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S):	Hersent		
SERIAL NO.:	Not Yet Assigned	GROUP NO.:	Not Yet Assigned
FILING DATE:	June 14, 2001	EXAMINER:	Not Yet Assigned
TITLE:	Method of Transporting Packets Between an Access Interface of a Subscriber Installation and a Shared Network, and Access Interface Implementing Such Method		

Assistant Commissioner for Patents
Washington, D.C. 20231
Box PCT, Attention Elected Office

PRELIMINARY AMENDMENT

Sir:

Please enter this Preliminary Amendment for the above-identified national phase application.

AMENDMENT

In The Title:

Please cancel the English version of the title of the invention as printed in the front page of the PCT publication, and substitute therefor:

-- METHOD OF TRANSPORTING PACKETS BETWEEN AN ACCESS INTERFACE OF A SUBSCRIBER INSTALLATION AND A SHARED NETWORK, AND ACCESS INTERFACE IMPLEMENTING SUCH METHOD --

In The Specification:

Page 4, between lines 18 and 19, insert the heading:

-- BRIEF DESCRIPTION OF THE DRAWINGS --

Page 4, between lines 31 and 32, insert the heading:

-- DESCRIPTION OF PREFERRED EMBODIMENTS --

In the Abstract:

Please cancel the Abstract as printed in the front page of the PCT publication, and insert therefor the following Abstract.

-- ABSTRACT

For transporting packets between an access interface of a subscriber installation and a concentrating router of a shared network the access interface carries out control operations on streams of packets transmitted to the concentrating router, within the framework of a contract between the subscriber and a manager of the shared network. After having carried out the control operations concerning a packet to be transmitted, the access interface transmits this packet to the concentrating router with a signature based on a secret shared with the concentrating router, authenticating that the packet has been subjected to the control operations. --

In the Claims:

Please amend Claims 1-10 to read as follows. A set of amended claims, red-lined to show the amendments, is attached hereto.

1. (Amended) A method of transporting packets between an access interface of a subscriber installation and a concentrating router of a shared network, comprising the steps of:

carrying out, at the access interface, control operations on streams of packets transmitted to the concentrating router, within the framework of a contract between the subscriber and a manager of the shared network, and

after having carried out the control operations concerning a packet to be transmitted, transmitting said packet from the access interface to the concentrating router with a signature based on a secret shared with the concentrating router, authenticating that the packet has been subjected to the control operations.

2. (Amended) A method according to claim 1, wherein the signature consists of a code word added to the content of the packet.

3. (Amended) A method according to claim 2, wherein said code word is calculated by hashing at least part of a content of the packet, involving the shared secret.

4. (Amended) A method according to claim 1, wherein the signature consists of an enciphering of a content of the packet by means of a private key forming said shared secret.

5. (Amended) A method according to claim 1, wherein the obtaining of the signature and at least some of the control operations are carried out within a single integrated circuit, without physical access immediately upstream of the obtaining of the signature.

6. (Amended) An access interface for linking an access router of a subscriber installation to a concentrating router of a shared network, comprising:

means for controlling streams of packets transmitted to the concentrating router, within the framework of a contract between the subscriber and a manager of the shared network, and

signature means receiving the packets delivered by the stream control means and producing signed packets transmitted to the concentrating router, each signed packet comprising a signature based on a secret shared with the concentrating router, authenticating that the packet has been subjected to the stream control means.

7. (Amended) An interface according to claim 6, wherein the signature consists of a code word added to the content of the packet.

8. (Amended) An interface according to claim 7, wherein the signature means include means for calculating said code word by hashing at least part of a content of the packet, involving the shared secret.

9. (Amended) An interface according to claim 6, wherein the signature consists of an enciphering of a content of the packet by means of a private key forming said shared secret.

10. (Amended) An interface according to claim 6, wherein the signature means and at least part of the stream control means belong to a single integrated circuit, without physical access between the stream control means and the signature means.

REMARKS

The present application is a national phase filing under 35 U.S.C. 371 of PCT/FR99/03097. PCT/FR99/03097 claims priority to FR No. 98/15756 filed on December 14, 1998, as indicated on the PCT cover page of the international application, as filed in French, submitted herewith.

Applicant submits that the present amendments introduce no new matter. Claims 1-10 are pending in the application. The Examiner is invited to call the undersigned, if the Examiner believes that a telephone conversation could be helpful in expediting prosecution of the instant application..

Respectfully submitted,

Pat LH Wall

Date: June 14, 2001
Reg. No. 41,418

Patrick R. H. Waller
Agent for Applicant(s)
Testa, Hurwitz, & Thibeault, LLP
High Street Tower
125 High Street
Boston, Massachusetts 02110

Tel. No.: (617) 248-7240
Fax No.: (617) 248-7100

2115181

Docket No. 2115.2000-000

CLAIM AMENDMENTS (RED-LINED VERSION)

1. (Amended) A [M]method of transporting packets between an access interface [(16)] of a subscriber installation [(13)] and a concentrating router [(12)] of a shared network [(10), characterized in that the access interface carries out] , comprising the steps of:

carrying out, at the access interface, control operations on streams of packets transmitted to the concentrating router, within the framework of a contract between the subscriber and a manager of the shared network, and [in that]

after having carried out the control operations concerning a packet to be transmitted, [the access interface transmits this] transmitting said packet from the access interface to the concentrating router with a signature based on a secret shared with the concentrating router, authenticating that the packet has been subjected to the control operations.

2. (Amended) A [M]method according to claim 1, [in which] wherein the signature consists of a code word added to the content of the packet.

3. (Amended) A [M]method according to claim 2, [in which] wherein said code word is calculated by [a technique of] hashing [a part] at least part of [the] a content of the packet, involving the shared secret.

4. (Amended) A [M]method according to claim 1, [in which] wherein the signature consists of an enciphering of [the] a content of the packet [with the aid] by means of a private key forming said shared secret.

5. (Amended) A [M]method according to [any one of claims 1 to 4, in which] claim 1, wherein the obtaining of the signature and [certain] at least some of the control operations are carried out within [one and the same] a single integrated circuit, without physical access immediately upstream of the obtaining of the signature.

6. (Amended) An [A]access interface for linking an access router [(15)] of a subscriber installation [(13)] to a concentrating router [(12)] of a shared network [(10), characterized in that it comprises] , comprising:

means [(39)] for controlling streams of packets transmitted to the concentrating router, within the framework of a contract between the subscriber and a manager of the shared network, and

signature means [(40)] receiving the packets delivered by the stream control means and producing signed packets transmitted to the concentrating router, each signed packet comprising a signature based on a secret shared with the concentrating router, authenticating that the packet has been subjected to the stream control means.

7. (Amended) An [I]interface according to claim 6, [in which] wherein the signature consists of a code word added to the content of the packet.

8. (Amended) An [I]interface according to claim 7, [in which] wherein [said code word is calculated by] the signature means [(40)] include means for calculating said code word by [a technique of] hashing [a part] at least part of [the] a content of the packet, involving the shared secret.

9. (Amended) An [I]interface according to claim 6, [in which] wherein the signature consists of an enciphering of [the] a content of the packet [with the aid] by means of a private key forming said shared secret.

10. (Amended) An [I]interface according to [any one of claims 6 to 9, in which] claim 6, wherein the signature means [(40)] and [a part] at least part of the stream control means [(39) form part of one and the same] belong to a single integrated circuit, without physical access between the stream control means and the signature means.

EXPRESS MAIL MAILING LABEL
No. EL280660416US

09/868151
JC03 Rec'd PCT/PTO 14 JUN 2001

METHOD OF TRANSPORTING PACKETS BETWEEN AN ACCESS INTERFACE OF A SUBSCRIBER INSTALLATION AND A SHARED NETWORK, AND ACCESS INTERFACE IMPLEMENTATING SUCH A METHOD

The present invention relates to packet based transmission networks. It applies in particular, but not exclusively, to shared networks operating according to the Internet protocol (IP).

The implementation of the invention comes within the framework of contractual relations between a provider of access to the shared network and his customers. The provider is furnished, for the attachment of the installations of his customers, with one or more concentrating routers for the shared network. Transmission lines link this concentrating router to the access interfaces of the customers' installations, which may be private network access router interfaces.

Here, the expression "police" functions designates various processing or control operations performed at the level of an interface of the network on data streams which pass through it. By way of nonlimiting examples, mention may be made of the counting of the packets exchanged between a given source address and a given destination address, the allocating of priorities to certain packets, address translations, the selective destruction of certain packets, etc.

These police functions may be included within a contractual framework between a subscriber (customer) and a manager of the network (provider of services). Such may for example be the case with functions relating to billing, to flow control, to authorization for access to certain sites linked to the network, to the implementing of reservation protocols such as RSVP, etc. They may also be included within the framework of

the internal organization of a public or private network, for example to control certain accesses.

Customarily, the police functions pertaining to the contractual framework between the access provider and his customers are implemented at the level of the concentrating router's attachment interfaces. This router hosts software for controlling the streams which travel around its various interfaces. The packets having certain originating or destination addresses or ports are counted, filtered, rearranged etc. according to the type of service offered. Owing to the large number of installations which may be linked to the concentrating router and to the variety of services which may be rendered in respect of these installations, the various stream controls to be applied may considerably increase the complexity of the router. This drawback is all the more noticeable as more and more diverse processing operations are requested by customers or required by new reservation protocols.

Moreover, this organization is not flexible for the customer who wishes to tailor certain characteristics of the service offered to him. To do this he must turn to his provider so that the latter may make the changes required at the level of his concentrating router.

An aim of the present invention is to propose a mode of operation of the network which enables a wide diversity of stream controls to be taken into account without resulting in an excessive increase in the complexity of the concentrating routers, and with a relative flexibility of configuration.

The invention thus proposes a method of transporting packets between an access interface of a subscriber installation and a concentrating router of a shared network, in which the access interface carries out control operations on streams of packets

transmitted to the concentrating router, within the framework of a contract between the subscriber and a manager of the shared network. After having carried out the control operations concerning a packet to be transmitted, the access interface transmits this packet to the concentrating router with a signature based on a secret shared with the concentrating router, authenticating that the packet has been subjected to the control operations.

Preferably, the obtaining of the signature and certain at least of the control operations are carried out within one and the same integrated circuit, without physical access immediately upstream of the obtaining of the signature.

The steam controls pertaining to the contractual framework between the manager of the network and the subscriber are thus decentralized, thereby avoiding the need for the concentrating router to take on all the diversity of the operations demanded by the various subscriptions. The mechanism for signing the packets guarantees to the manager of the network that the subscriber, who is furnished with the access interface at his premises, does not send him packets which have not been subjected to the stream control operations, that is to say which have sidestepped the police and billing functions.

The method gives rise to a distributed architecture of access and of concentration, which is well suited to taking account of the increases in traffic and in diversity of services which future applications will entail.

The subscriber benefits moreover from greater flexibility for dynamically defining the characteristics of his subscription. He merely needs to intervene at the level of the access interface with which he is furnished. He may moreover define the police functions pertaining to the contractual

framework with the access provider on the same platform as the other police functions which he uses for the internal organization of his installation, thereby simplifying organization thereof.

Another aspect of the present invention concerns an access interface for linking an access router of a subscriber installation to a concentrating router of a shared network, comprising means for controlling streams of packets transmitted to the concentrating router, within the framework of a contract between the subscriber and a manager of the shared network, and signature means receiving the packets delivered by the stream control means and producing signed packets transmitted to the concentrating router, each signed packet comprising a signature based on a secret shared with the concentrating router, authenticating that the packet has been subjected to the stream control means.

Other features and advantages of the present invention will become apparent in the following description of nonlimiting exemplary embodiments, with reference to the appended drawings, in which:

- figure 1 is a diagram of a network where the invention may be implemented;
- figure 2 is a schematic diagram of an access router of a private installation of this network;
- figure 3 is a schematic diagram of a stream processing device forming part of an interface of the router of figure 2; and
- figure 4 is a graph of elementary processing operations undertaken by the device of figure 3.

Figure 1 shows a wide area shared network (WAN) 10 comprising a certain number of interconnected routers and switches 11, 12. The case where the shared network 10 operates according to the IP protocol is considered here. A certain number of the routers are

concentrating routers 12 to which private installations 13 are linked.

A private subscriber installation 13 is typically linked to the shared network 10 by means of an access router 15, one of whose interfaces 16 is linked to a line 17 for transmission from and to the concentrating router 12. The access router 15 can be linked to other routers of the private installation 13 or to servers or terminals 18 of this installation, by means of other interfaces, which are not represented in figure 1.

Figure 2 shows an exemplary architecture of the access router 15. The outside interface 16, and also the interfaces 20, 21 with the remainder of the private installation 13, are linked to the core of the router consisting of a packet forwarding engine 22. The forwarding engine 22 forwards the packets from one interface to another on the basis of the address fields and port fields contained in the headers of the packets in accordance with the IP protocol and with any extensions thereof (TCP, UDP, etc), by referring to routing tables.

Certain of the interfaces of the access router 15 are provided, in just one or in both directions of transmission, with processing devices, or stream processors, 24, 25 undertaking police functions. In the illustrative example of figure 2, the device 24 is fitted to the outside interface 16 in the outgoing direction, and the device 25 is fitted to another interface 20 in the incoming direction.

The access router is supervised by a management unit 26 which can consist of a microcomputer or a work station which executes routing software serving in particular to configure the routing table of the forwarding engine 22 and the stream processors 24, 25 and to exchange control or protocol information with

them. These commands and exchanges are effected by way of an appropriate software programming interface (API).

Most of the existing packet routing and forwarding software is readily available in the Unix environment, but its performance is customarily limited on account of the frequent interruptions of the operating system. It is much faster to use a real time operating system such as VxWorks, but this complicates the implementation of the routing software.

The role of the stream processors 24, 25 is to assist the non-real time operating system (such as Unix), on the basis of which the management unit 26 functions, in the complex tasks for manipulating the streams which require real time performance (forwarding, filtering, enciphering, etc.). These processors implement a certain number of tools for manipulating the streams which may be linked dynamically according to any combination so as to perform the task required. This configuration can be achieved through the Unix operating system by calling the API functions, thereby greatly facilitating the setting up of new functionalities by the programmer.

As illustrated diagrammatically by figure 1, one of the tasks performed by the stream processor 24 of the outside interface 16 of the access router 15 consists in transmitting each packet to the concentrating router 12 while appending a digital signature (block 40) thereto. This signature attests that the packets in question have been subjected to the other stream control operations (block 39) performed by the processor 24.

The corresponding interface 28 of the concentrating router 12 comprises a module for analyzing the packets received on the line 17 so as to make sure that the signature is present.

This signature technique advantageously makes it possible to decentralize the stream control

operations necessary for the contractual relations between the manager of the concentrating router 12, which provides the service of attachment to the shared network 10, and the subscribers whose installations 13 are linked to this concentrating router 12. In the conventional embodiments, these stream control operations are performed at the level of the concentrating router. This results in considerable complexity of the concentrating router when it is attached to a fairly large number of private installations, and a lack of flexibility for the subscribers when modifications are required.

By performing these stream control operations at the level of the access routers 15, great flexibility is afforded in this regard. The signing of the packets then guarantees to the service provider that the line 17 does not send him valid packets which depart from the contractual framework with the subscriber. If such a packet were to appear, the interface 28 of the concentrating router 12 would simply eliminate it after having noted the absence of the appropriate signature.

Various conventional processes may be used to construct and analyze the signature of the packets, on the basis of a secret shared between the routers 12 and 15. The signature can in particular have the form of a code word added to the content of the packet, and calculated on the basis of all or part of this content and of a secret key, the calculation being performed with the aid of a function which is extremely difficult to invert in order to recover the secret key. It is thus possible to use a technique of hashing the content of the packet, or of just a part of this content, for example an MD5 hashing (see R. Rivest, RFC 1231, "The MD5 Message Digest Algorithm").

It is also possible to use an enciphering process to form the signature of the packets. The

content of the packet is then enciphered with the aid of a private key, the interface 28 of the concentrating router undertaking the corresponding deciphering with the aid of a public or private key. The unenciphered packets, or those enciphered by means of a wrong key are then destroyed at the level of the interface 28.

As an option, provision may be made for the interface 28 of the concentrating router to also sign the packets which it transmits on the line 17, and for the interface 16 of the access router to verify this signature so as to make sure that the packets received are valid.

Figure 3 shows the organization of a stream processor 24 or 25 of an interface of the access router 15.

The stream processor receives a sequence of incoming packets 30 each comprising a header 31 in accordance with the IP protocol, and delivers a sequence of outgoing packets 32 having a header 33 after having performed certain elementary processing operations whose nature depends on the data streams concerned.

The incoming packets 30 are stowed away in a packets memory 35 organized as a first in-first out (FIFO) stack. Each packet is fed to the memory 35 with a processing label 36. The processing label initially has a specified value (0 in the example represented) for the incoming packets 30.

The stream processor is supervised by a unit 37 which cooperates with a table 38 making it possible to associate a particular processing module with each value of the processing label. In the simplified example represented in figure 3, the stream processor comprises an assembly of five processing modules M1 - M5 effecting elementary processing operations of different kind.

After the execution of an elementary processing operation, the supervisory unit 37 consults the packets memory 35. If the latter is not empty, a packet is extracted therefrom according to the FIFO organization. The supervisory unit 37 consults the table 38 to determine which processing module corresponds to the label of this packet. The unit 37 then activates the module in question so that it performs the corresponding elementary processing operation. In certain cases, this elementary processing operation may entail a modification of the content of the packet, in particular its header.

It will be understood that the "extraction" of the packet, to which reference is made, is an extraction in the logical sense from the FIFO memory. The packet is not necessarily removed from the memory. The addresses of the packets in the memory 35 can be managed in a conventional manner by means of pointers so as to comply with the FIFO organization. The activated processing module can be furnished simply with the address of the current packet so as to perform the required reads, analyses, modifications or deletions as appropriate.

The first processing module M1, associated with the initial label 0, is a filtering module which analyzes the address field and/or protocol definition field and/or port field of the IP header of the packets. With the help of an association table T1, the filtering module M1 delivers a second processing label which identifies a string of elementary processing operations which will subsequently have to be performed on the packet. After having determined the second processing label for the packet extracted from the memory 35, the filtering module M1 stows away the packet in the memory 35 again, with the second processing label. The next elementary processing

operation will then be executed when the packet is again extracted from the memory.

The module M2 is a module for counting the packets relating to certain streams. In the case of the association table 38 represented in figure 3, this module M2 is called for the processing labels 2 and 4. When it processes a packet, the module M2 increments a counter with the number of bytes of the packet, or else with the value 1 in the case of a packets counter. The counter can be made secure, in particular if it serves for the billing of the subscriber by the manager of the network 10. In the case of a secure counter, requests are regularly made to the access provider to obtain transmission credits, the relevant packets being destroyed if the credit is used up.

The module M3 of figure 3 is a priorities management module. In the case of the association table 38 represented in figure 3, this module M3 is called for the processing label 3. The module M3 operates on the TOS ("Type of Service") field of the IP header of the packets. The TOS is used in the network to manage forwarding priorities so as to provide a certain quality of service on certain links. The TOS field can be changed according to prerecorded tables. These tables can be defined under the control of the access provider so as to prevent packets being inappropriately transmitted with a high priority, which might disturb the network.

The elementary processing operation performed last on a packet of the memory 35 is either its destruction (module M4 activated by the label 8), or its resubmission to the output of the stream processor (module M5 activated by the label 5 or 9). The module M4 can be used to destroy packets having a certain destination and/or a certain origin.

The modules M2 and M3, which do not terminate the processing operations to be undertaken in respect

of a packet (except in the case of destruction), each operate with a label translation table T2, T3. This translation table designates, for the processing label extracted from the memory 35 with the current packet, another processing label designating the next elementary processing operation to be undertaken. The elementary processing operation undertaken by this module M2 or M3 terminates with the associating of the packet with this other processing label and the reinjecting of the packet thus processed into the memory 35.

In this way, highly varied combinations of processing operations can be performed on the various data streams passing through the processor.

Figure 4 shows a simplified example corresponding to the tables 38, T1 - T3 represented in figure 3. The incoming packet 30, associated with the first label 0, is firstly subjected to the filtering effected by the module M1.

In the particular case considered, the stream processor 24 counts the packets transmitted from a source address AS1 to a destination address AD1 and a port P1, and modifies the TOS field of these packets before delivering them on the line 17, this corresponding to the upper branch of the graph of figure 4. Moreover, the stream processor 24 counts the packets emanating from a source address AS2 heading for a port P2 before destroying them, this corresponding to the lower branch of figure 4. The other packets are simply delivered to the line 17. The default value (9) of the processing label returned by the module M1 therefore simply designates the output module M5. If the module M1 detects in the packet extracted from the memory 35 the combination AS1, AD1, P1 in the relevant address and port fields, it returns the packet with the processing label 2. If the values AS2, P2 are detected

in the address and port fields, it is the label 4 which is returned with the packet.

These labels 2 and 4 both correspond to the counting module M2. The label will also designate for this module the memory address of the counter which has to be incremented. The table T2 with which the module M2 operates will make it possible at the end of processing to perform the return to the next module to be activated (M3 designated by the label 3 for the packets whose TOS has to be changed, M4 designated by the label 8 for the packets to be destroyed).

The module M3 receives packets with the processing label 3, and returns them with the label 9 after having made the required modification of the TOS field.

From this simplified example it can be seen that the stream processor makes it possible, through the identification of a stream by the filtering module M1, to perform various combinations of elementary processing operations in a relatively simple and fast manner.

A main advantage of this way of proceeding is the flexibility of the operations for configuring the stream processor. The tables 38, T1 - T3 which define any graph of elementary processing operations, such as the one represented in figure 4, can be constructed relatively simply and with a small real time constraint by means of the management unit 36 through the API. The same holds in respect of the information enabling the modules M1 - M5 to perform their elementary processing operations (description of the counts to be performed by the module M2, way of changing the TOS fields by the module M3, etc.).

In practice, the stream processor may comprise various processing modules other than those represented by way of example in figures 3 and 4, according to the requirements of each particular installation (for

example, module for managing the output queues, address translation module, etc.)

The function of signing the packets transmitted, which was described earlier, can form part of the elementary processing undertaken by the output module M5. In a typical embodiment of the access router, the stream processor 24 will be included in an application specific integrated circuit (ASIC) organized around a microcontroller core. This embodiment allows there to be no physical access between the stream control modules 39 (at least those which pertain to the relations between the subscriber and the manager of the network 10) and the module M5 which is responsible for signing the packets, corresponding to the block 40 of figure 1. This improves the security of the link from the viewpoint of the manager of the network.

Claims

1. Method of transporting packets between an access interface (16) of a subscriber installation (13) and a concentrating router (12) of a shared network (10), characterized in that the access interface carries out control operations on streams of packets transmitted to the concentrating router, within the framework of a contract between the subscriber and a manager of the shared network, and in that after having carried out the control operations concerning a packet to be transmitted, the access interface transmits this packet to the concentrating router with a signature based on a secret shared with the concentrating router, authenticating that the packet has been subjected to the control operations.

2. Method according to claim 1, in which the signature consists of a code word added to the content of the packet.

3. Method according to claim 2, in which said code word is calculated by a technique of hashing a part at least of the content of the packet, involving the shared secret.

4. Method according to claim 1, in which the signature consists of an enciphering of the content of the packet with the aid of a private key forming said shared secret.

5. Method according to any one of claims 1 to 4, in which the obtaining of the signature and certain at least of the control operations are carried out within one and the same integrated circuit, without physical access immediately upstream of the obtaining of the signature.

6. Access interface for linking an access router (15) of a subscriber installation (13) to a concentrating router (12) of a shared network (10),

characterized in that it comprises means (39) for controlling streams of packets transmitted to the concentrating router, within the framework of a contract between the subscriber and a manager of the shared network, and signature means (40) receiving the packets delivered by the stream control means and producing signed packets transmitted to the concentrating router, each signed packet comprising a signature based on a secret shared with the concentrating router, authenticating that the packet has been subjected to the stream control means.

7. Interface according to claim 6, in which the signature consists of a code word added to the content of the packet.

8. Interface according to claim 7, in which said code word is calculated by the signature means (40) by a technique of hashing a part at least of the content of the packet, involving the shared secret.

9. Interface according to claim 6, in which the signature consists of an enciphering of the content of the packet with the aid of a private key forming said shared secret.

10. Interface according to any one of claims 6 to 9, in which the signature means (40) and a part at least of the stream control means (39) form part of one and the same integrated circuit, without physical access between the stream control means and the signature means.

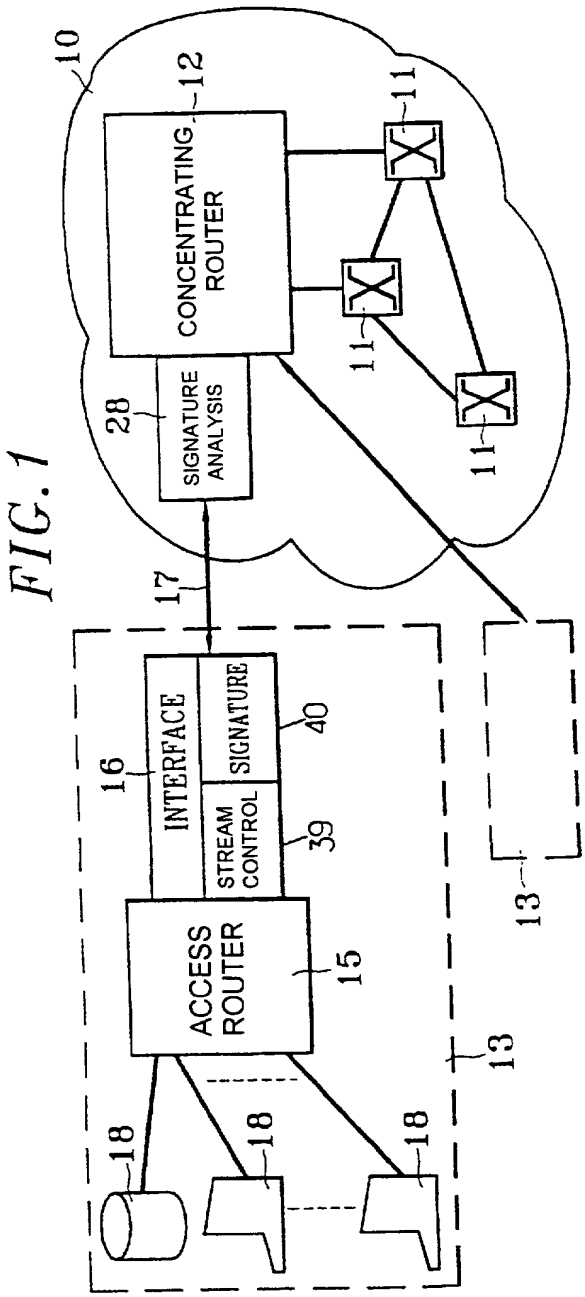

10
12
CONCENTRATING ROUTER
11
11
11
28
SIGNATURE ANALYSIS
17
16
INTERFACE
SIGNATURE
40
STREAM CONTROL
39
ACCESS ROUTER
15
18
18
18
13
13

FIG. 1

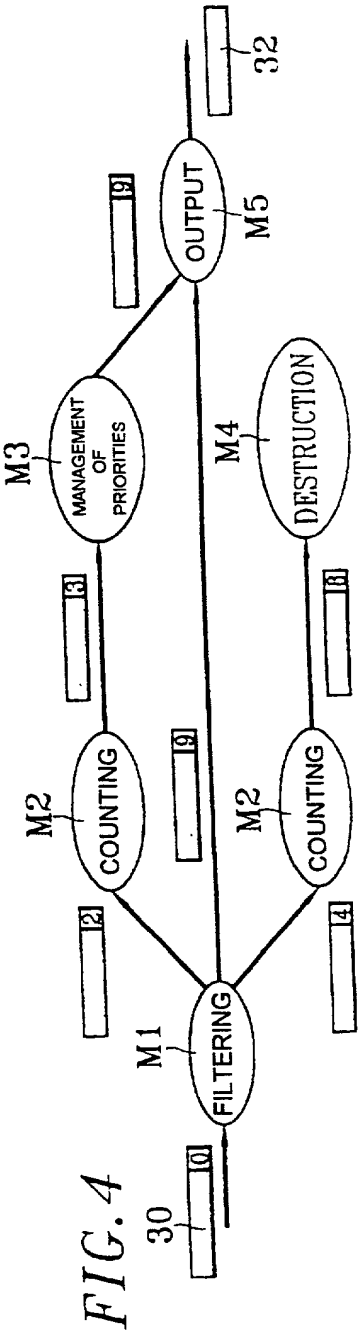

32
OUTPUT
M5
19
M3
MANAGEMENT OF PRIORITIES
M4
DESTRUCTION
13
18
M2
COUNTING
19
M2
COUNTING
12
14
M1
FILTERING
10
30

FIG. 4

FIG.2

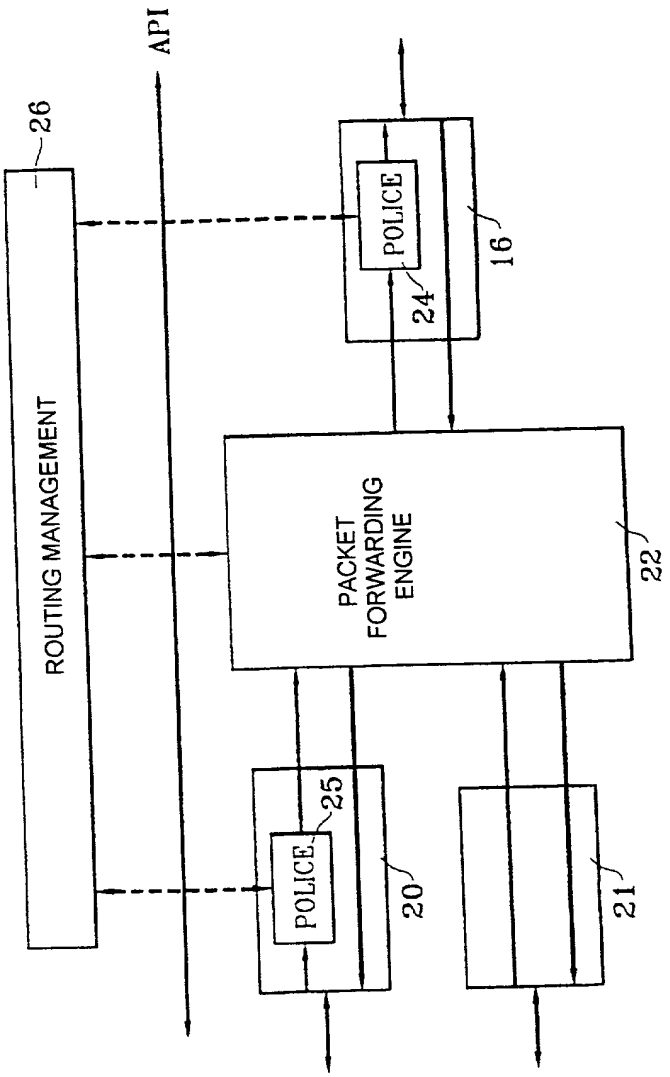
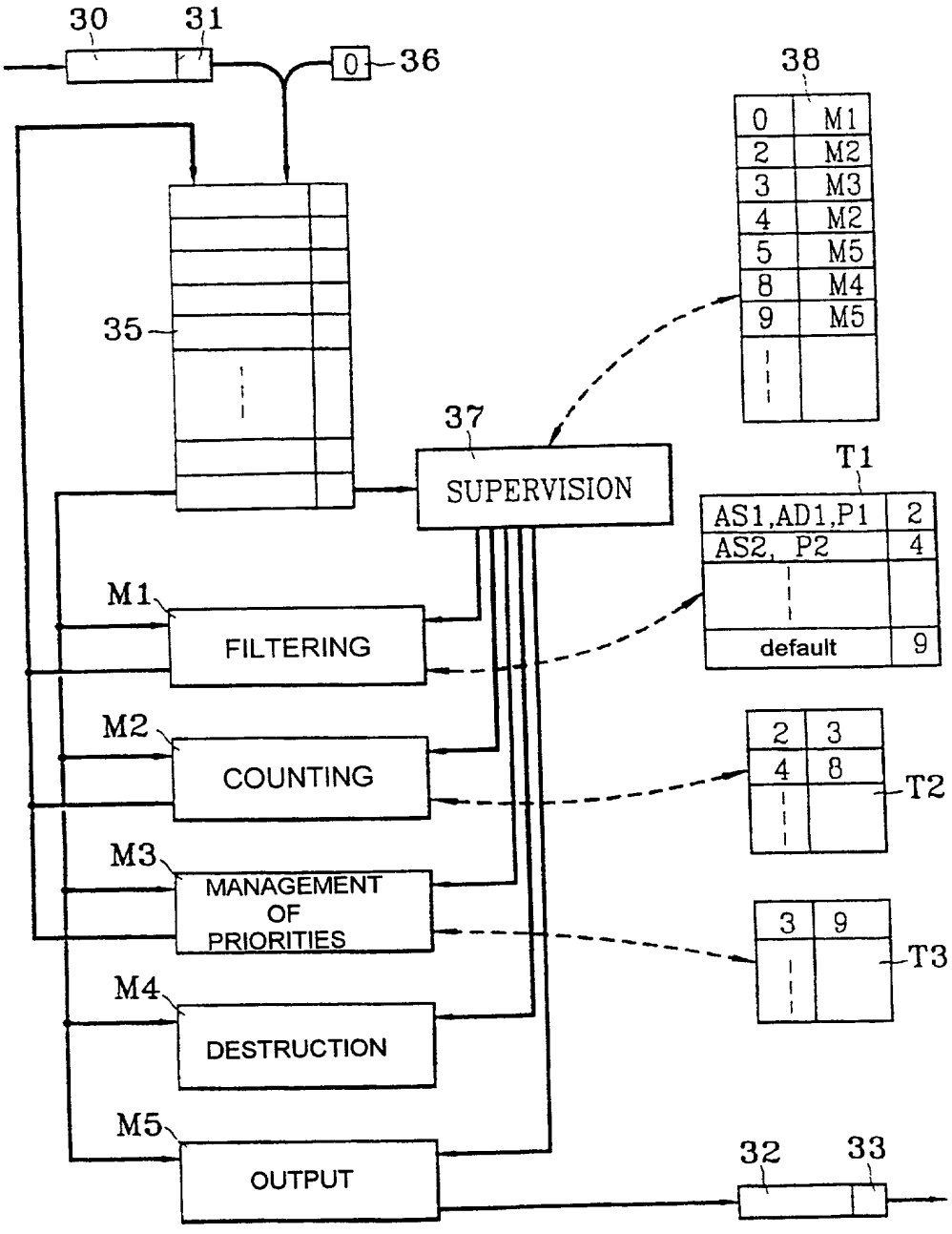

API
26
ROUTING MANAGEMENT
POLICE
24
16
PACKET
FORWARDING
ENGINE
22
POLICE
25
20
21

FIG.3


30
31
0
36
38
0 M1
2 M2
3 M3
4 M2
5 M5
8 M4
9 M5
35
37
SUPERVISION
T1
AS1,AD1,P1 2
AS2, P2 4
default 9
M1
FILTERING
M2
COUNTING
2 3
4 8
T2
M3
MANAGEMENT OF PRIORITIES
3 9
T3
M4
DESTRUCTION
M5
OUTPUT
32
33

Title: Method of Transporting Packets Between an Access Interface of a Subscriber Installation and a Shared Network, and Access Interface Implementing Such Method
Inventor(s): Hersent
Serial No. Not Yet Assigned
Atty Docket No. NCX-002
Express Mail Mailing Label No. EL280660416US

09/868151

10/27/01 15:39:50

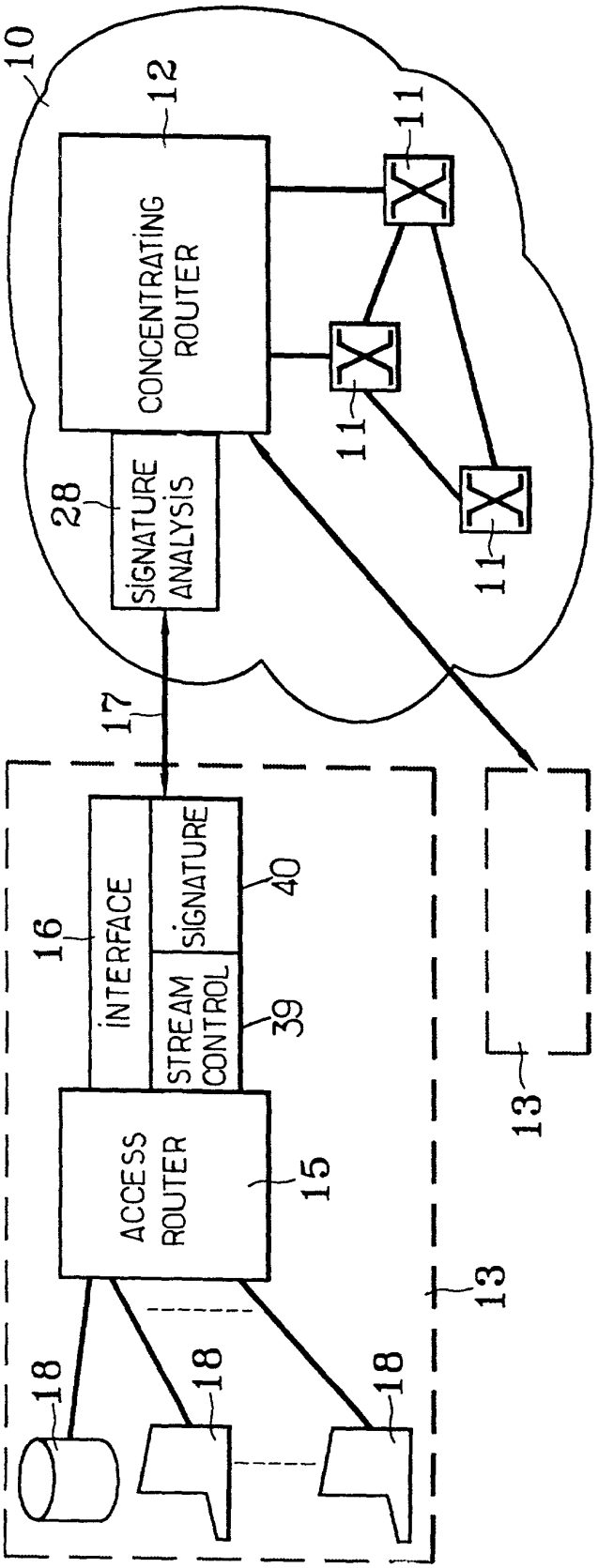


FIG. 1

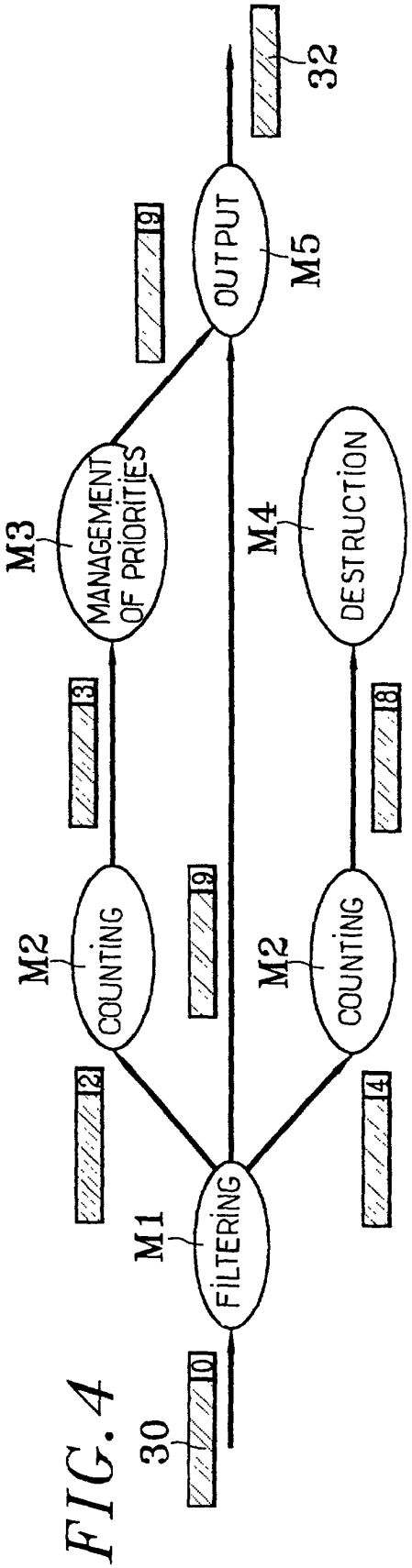


FIG. 4

09/868151

PCT/FR99/03150

FIG. 2

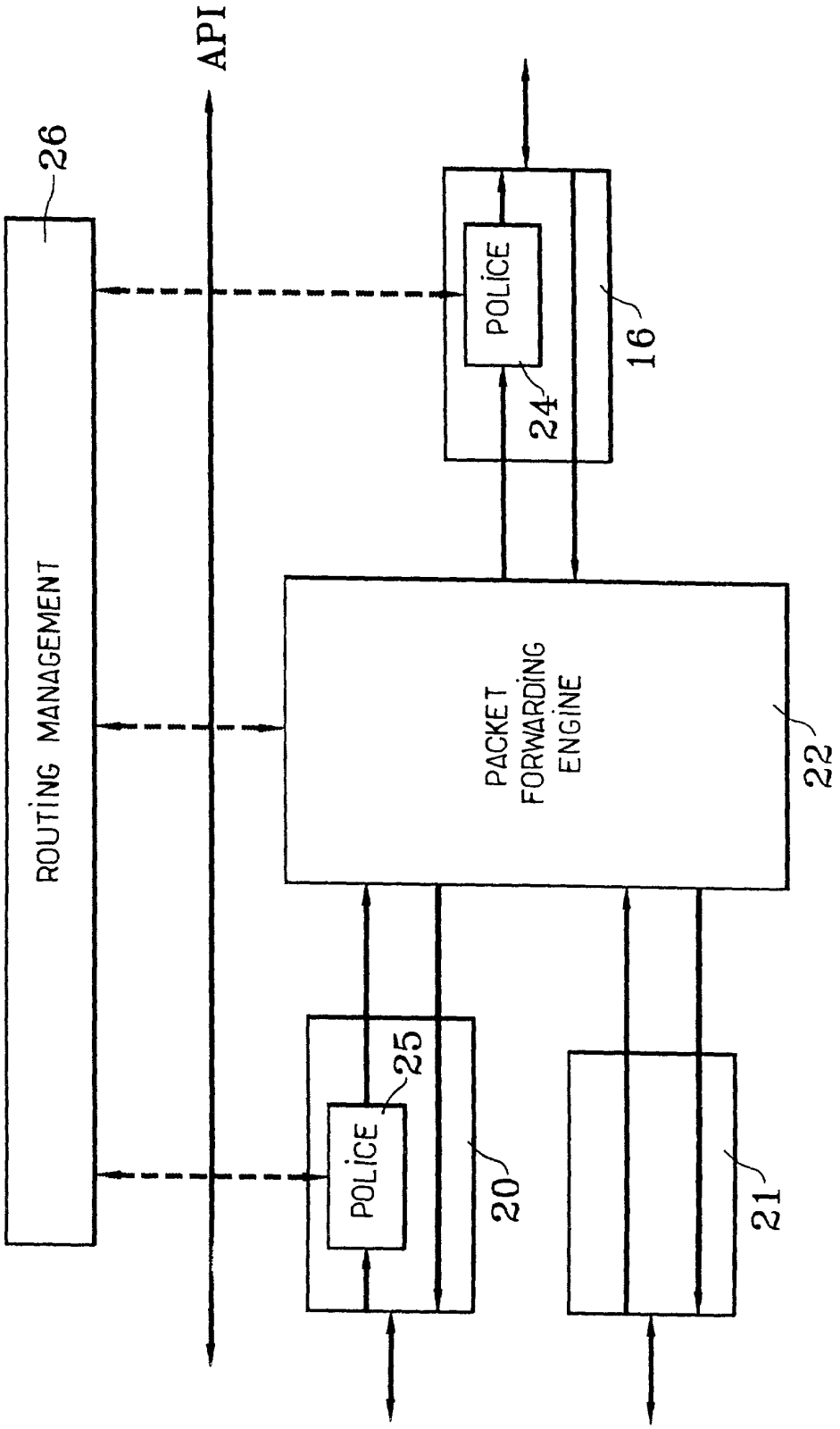
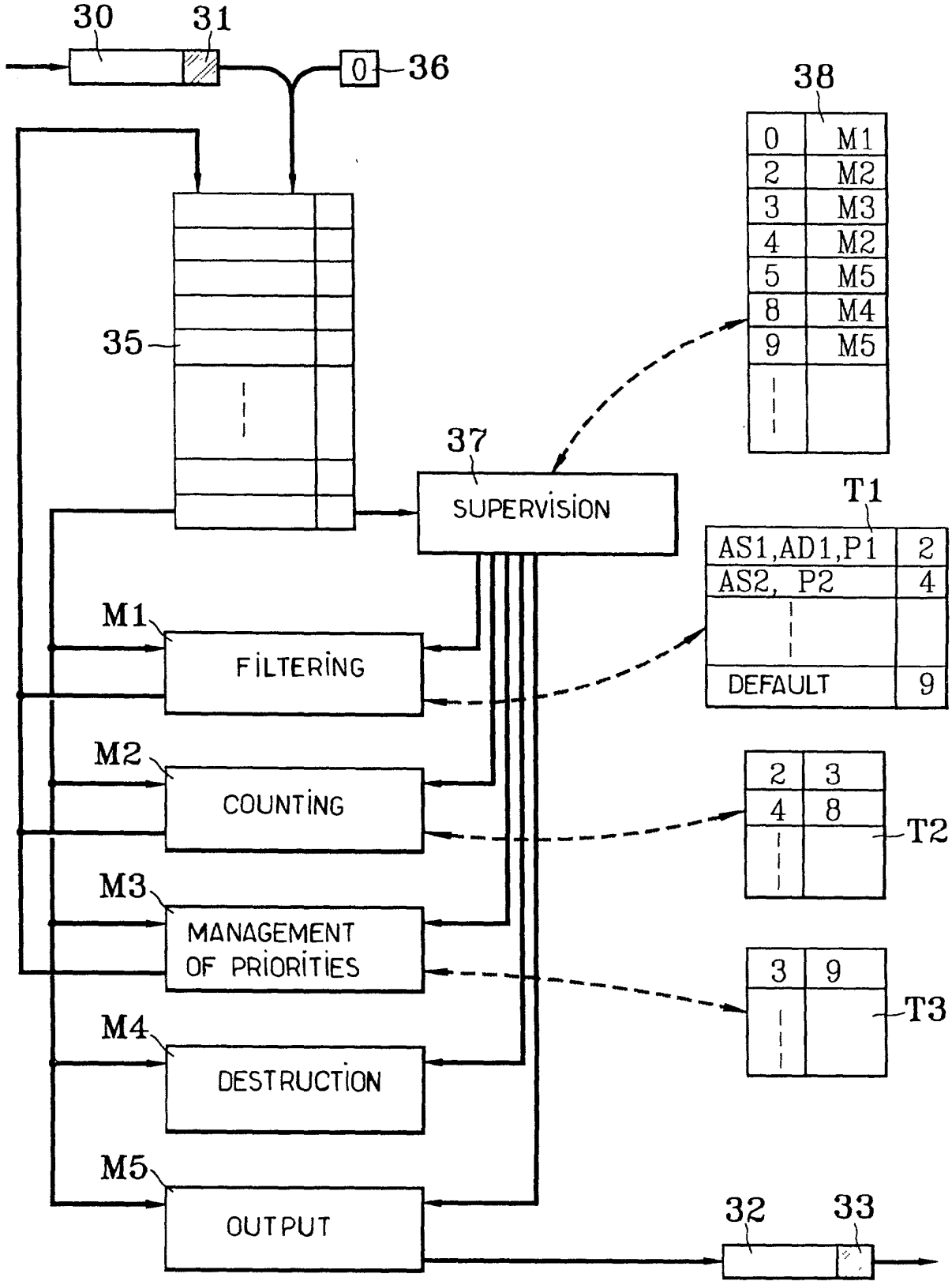


FIG.3



09868151 - 102704

EXPRESS MAIL MAILING LABEL

No. EL902309545US

Rec'd PCT/PTO 17 OCT 2001

09/868,151

DECLARATION AND POWER OF ATTORNEY FOR UTILITY OR DESIGN PATENT APPLICATION		
☐ Declaration Submitted with Initial Filing ☒ Declaration Submitted after Initial Filing (surcharge 37 CFR 1.16(e) required)	Attorney Docket No.	NCX-002
	First Named Inventor	Olivier HERSENT
	COMPLETE IF KNOWN	
	Application Serial Number	09/868,151
	Filing Date	June 14, 2001
	Group Art Unit	
	Examiner Name	

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD OF TRANSPORTING PACKETS BETWEEN AN ACCESS INTERFACE OF A SUBSCRIBER INSTALLATION AND A SHARED NETWORK, AND ACCESS INTERFACE IMPLEMENTATING SUCH A METHOD

(Title of the Invention)

the specification of which

☒ is attached hereto

OR

☒ was filed on (MM/DD/YYYY) December 10, 1999 as United States Application Serial Number or PCT International Application Number PCT FR99/03097 and was amended on (MM/DD/YYYY) _____ *(if applicable).*

I hereby state that I have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose to the Patent Office all information known by me to be material to patentability as defined in 37 CFR 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
9815756	FRANCE	12/14/1998	☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application numbers are listed on a supplemental priority data sheet attached hereto.

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Serial Number(s)	Filing Date (MM/DD/YYYY)	
		☐ Additional provisional application serial numbers are listed on a supplemental priority data sheet attached hereto.

DECLARATION – Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365(c), of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Serial Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number *(if applicable)*
PCT FR99/03097	12/10/1999	

☐ Additional U.S. or PCT international application numbers are listed on a supplemental priority data sheet attached hereto.

As a named inventor, I hereby appoint the following registered practitioners to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: ☐ Customer Number

OR

☒ Registered practitioner(s) name/registration number listed below

Place Customer Number Bar Code Label Here

Name	Registration Number	Name	Registration Number
Michael J. Bastian	47,411	Kurt W. Lockwood	40,704
Steven M. Bauer	31,481	Thomas C. Meyers	36,989
Elias C. Behrakis	47,416	Joseph B. Milstein	42,897
John V. Bianco	36,748	David G. Miranda	42,898
Isabelle A.S. Blundell	43,321	Ronda P. Moore	44,244
Maureen A. Bresnahan	44,559	Indranil Mukerji	P-46,944
Michael H. Brodowski	41,640	Edmund R. Pitcher	27,829
Jennifer A. Camacho	43,526	Michael A. Rodriguez	41,274
Joseph A. Capraro, Jr.	36,471	Jamie H. Rose	45,054
John J. Cotter	38,116	R. Stephen Rosenholm	45,283
John V. Forcier	42,545	Christopher W. Stamos	35,370
Steven J. Frank	33,497	Diana M. Steel	43,153
Kia L. Freeman	47,577	Joseph P. Sullivan	45,349
Brian M. Gaff	44,691	Robert J. Tosti	35,393
Michael J. Giannetta	42,574	Thomas A. Turano	35,722
Duncan A. Greenhalgh	38,678	Christine C. Vito	39,061
William G. Guerin	41,047	Patrick R.H. Waller	41,418
Jonathan A. Harris	44,744	Daniel A. Wilson	45,508
Ira V. Heffan	41,059	Gerald E. Worth	45,238
Danielle L. Herritt	43,670	Yin P. Zhang	44,372
Douglas J. Kline	35,574		
John D. Lanza	40,060		

☐ Additional registered practitioners named on supplemental Registered Practitioner Information sheet attached hereto.

Direct all correspondence to:

Patent Administrator
Testa, Hurwitz & Thibeault, LLP
High Street Tower
125 High Street
Boston, MA 02110
Tel. No.: (617) 248-7000
Fax No.: (617) 248-7100

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor:	☐ A petition has been filed for this unsigned inventor						
Given Name (first and middle [if any])			Family Name or Surname				
Olivier			HERSENT				
Inventor's Signature					Date	19-06-01	
Residence	City		State		Country		Citizenship	FRENCH
Mailing Address	9 Bld Detolle, Résidence Olympia, 1400 CAEN						
Mailing Address (ln. 2)	City		State		ZIP		Country	FRANCE

☐ Additional inventors are being named on the ____ supplemental Additional Inventor(s) sheet(s) attached hereto.

Name of Additional Joint Inventor, if any:	☐ A petition has been filed for this unsigned inventor						
Given Name (first and middle [if any])			Family Name or Surname				
Inventor's Signature					Date		
Residence	City		State		Country		Citizenship	
Mailing Address							
Mailing Address (ln. 2)	City		State		ZIP		Country	

Name of Additional Joint Inventor, if any:	☐ A petition has been filed for this unsigned inventor						
Given Name (first and middle [if any])			Family Name or Surname				
Inventor's Signature					Date		
Residence	City		State		Country		Citizenship	
Mailing Address							
Mailing Address (ln. 2)	City		State		ZIP		Country	